

## CLAIM LISTING

1. (original): A method comprising:

forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a  
licensing server; and

the persistent license includes a key that is encrypted such that the  
key is not accessible by the client; and

receiving a license in response to the request, wherein the received license  
includes the key that is:

accessible by the client; and

for accessing the encrypted content.

2. (original): A method as described in claim 1, further comprising:

forming an initial request for:

communication to the licensing server; and

storing encrypted content by the client;

receiving the persistent license at the client in response to the initial  
request; and

storing the encrypted content and the persistent license by the client.

3. (original): A method as described in claim 1, further comprising:

1 forming an initial request by another client for:  
2 communication to the licensing server; and  
3 storing encrypted content by the other client;  
4 receiving the persistent license at the other client in response to the initial  
5 request;  
6 storing the encrypted content and the persistent license by the other client;  
7 and  
8 obtaining the persistent license by the client from the other client.  
9  
10

11 4. (original): A method as described in claim 1, wherein the received  
12 license is a boundary license and the key is a boundary key, and further  
13 comprising:

14 decrypting a session license utilizing a client key to obtain a session key;  
15 decrypting the boundary license utilizing the session key to obtain the  
16 boundary key;  
17 decrypting a content license utilizing the boundary key to obtain a content  
18 key; and  
19 decrypting the encrypted content utilizing the content key.  
20  
21

22 5. (original): A method as described in claim 4, wherein:  
23 the session license includes access rules for the client for a session initiated  
24 between the client and the licensing server;  
25

1 the boundary license includes access rules for the client for the encrypted  
2 content that is within a rights boundary in the encrypted content; and

3 the content license includes access rules for the client for the encrypted  
4 content.

5  
6 6. (original): A method as described in claim 4, wherein:

7 the persistent license was encrypted using an asymmetric encryption  
8 algorithm; and

9 the encrypted content, the boundary license, and the content license were  
10 encrypted using respective symmetric encryption algorithms.

11  
12  
13 7. (original): A method as described in claim 1, further comprising:

14 decrypting a session license utilizing a client key to obtain a session key,  
15 wherein the session license includes access rules for a session initiated between  
16 the client and the licensing server;

17 decrypting the received license utilizing the session key to obtain a  
18 decrypted boundary license, wherein:

19 the received license is an encrypted boundary license and the key  
20 within the boundary license is a boundary key; and

21 the boundary license includes access rules for content within a rights  
22 boundary in the encrypted content that is at least one of a television  
23 program and a television channel;  
24  
25

1 decrypting a content license utilizing the boundary key to obtain a content  
2 key, wherein the content license includes access rules for the encrypted content;  
3 and

4 decrypting the encrypted content utilizing the content key, wherein the  
5 encrypted content includes at least a portion of a television broadcast.

6  
7 8. (original): A method as described in claim 1, wherein the key is for  
8 decrypting the encrypted content.  
9

10  
11 9. (original): A method as described in claim 1, wherein the encrypted  
12 content is streamed to the client.  
13

14 10. (original): One or more computer-readable media comprising  
15 computer-executable instructions that, when executed, perform the method as  
16 recited in claim 1.  
17

18  
19 11. (original): A method comprising:  
20 forming a request by a client for communication to a licensing server,  
21 wherein the request is for storing encrypted content by the client;  
22 receiving a persistent license at the client in response to the request,  
23 wherein:  
24

25 the persistent license includes a key that is encrypted;

1 the key, when decrypted, provides access to the encrypted content;  
2 the key is configured to be decrypted by the licensing server; and  
3 the client is not configured to decrypt the key from the persistent  
4 license; and  
5 storing the persistent license and the encrypted content by the client.  
6

7  
8 12. (original): A method as described in claim 11, further comprising:  
9 forming a subsequent request by the client to access the stored content,  
10 wherein the subsequent request:

11 is for communication to the licensing server; and  
12 includes the persistent license; and  
13 receiving a second license at the client in response to the subsequent  
14 request, wherein:

15 the second license includes the key; and  
16 the second license is configured to be decrypted by the client such  
17 that the client obtains access to the key.  
18

19  
20 13. (original): A method as described in claim 11, further comprising:  
21 forming a subsequent request by another client to access the stored content,  
22 wherein the subsequent request:

23 is for communication to the licensing server; and  
24 includes the persistent license; and  
25

1 receiving a second license at the other client in response to the subsequent  
2 request, wherein:

3 the second license includes the key; and

4 the second license is configured to be decrypted by the other client  
5 such that the other client obtains access to the key.

6  
7 14. (original): A method as described in claim 11, wherein the  
8 encrypted content is streamed to the client.

9  
10 15. (original): A method as described in claim 11, wherein the license  
11 includes a certificate for verifying the licensing server by the client.

12  
13 16. (original): One or more computer-readable media comprising  
14 computer-executable instructions that, when executed, perform the method as  
15 recited in claim 11.

16  
17 17. (original): A method comprising:  
18  
19 forming a first request for communication to a licensing server, wherein the  
20 first request is for storing encrypted content;  
21  
22 receiving a persistent license in response to the request, wherein the  
23 persistent license includes a boundary key;  
24  
25 storing the persistent license and the content;

1 forming a second request to access the encrypted content, wherein the  
2 second request includes the persistent license;  
3 sending the second request to the licensing server;  
4 receiving a boundary license in response to the second request, wherein the  
5 boundary license includes the boundary key;  
6 decrypting the boundary license using a session key to obtain the boundary  
7 key;  
8 decrypting a content license using the boundary key to obtain a content key;  
9 and  
10 decrypting the encrypted content using the content key.

11  
12  
13 18. (original): A method as described in claim 17, wherein the forming  
14 of:

15 the first request is performed by a first client; and  
16 the second request is performed by a second client.

17  
18  
19 19. (original): A method as described in claim 17, wherein the first and  
20 second requests are formed by a client.

21  
22 20. (original): A method as described in claim 17, further comprising at  
23 least one of decoding the decrypted content and outputting the decoded content.  
24  
25

1 21. (original): A method as described in claim 17, wherein:

2 the persistent license was encrypted using an asymmetric encryption  
3 algorithm; and

4 the content, the boundary license, and the content license were encrypted  
5 using respective symmetric encryption algorithms.

6  
7 22. (original): One or more computer-readable media comprising  
8 computer-executable instructions that, when executed, perform the method as  
9 recited in claim 17.  
10

11  
12 23. (original): A client comprising:

13 a processor; and

14 memory configured to maintain:

15 a persistent license including a key that is encrypted; and

16 a playback application that is executable on the processor to:

17 form a request to access encrypted content, wherein the  
18 request:  
19

20 is for communication to a licensing server; and

21 includes the persistent license;

22 receive a response to the request that includes the key; and  
23 access the encrypted content utilizing the key.  
24  
25



1 24. (original): A client as described in claim 23, wherein the key is for  
2 decrypting the encrypted content.

3  
4 25. (original): A client as described in claim 23, wherein:  
5 the memory is further configured to maintain a content license;  
6 the key included in the persistent license is for decrypting the content  
7 license;  
8 the content license includes a content key; and  
9 the content key is for decrypting the encrypted content.  
10

11  
12 26. (original): A client as described in claim 23, wherein:  
13 the memory is further configured to maintain a content license;  
14 the key included in the persistent license is for decrypting the content  
15 license;  
16 the content license includes a content key;  
17 the content key is for decrypting the encrypted content; and  
18 the playback application is executable to:  
19 decrypt the content license using the key to obtain the content key;  
20 and  
21 decrypt the content using the content key.  
22  
23  
24

25 27. (original): A client as described in claim 23, wherein:

1 the memory is further configured to maintain a session license, a content  
2 license, and a client key;

3 the client key is for decrypting the session license;

4 the session license includes a session key for decrypting the response;

5 the response is a boundary license;

6 the key included in the response is a boundary key for decrypting the  
7 content license;

8 the content license includes a content key; and

9 the content key is for decrypting the encrypted content.  
10

11  
12 28. (original): A client as described in claim 23, wherein:

13 the memory is further configured to maintain a session license, a content  
14 license, and a client key;

15 the client key is for decrypting the session license;

16 the session license includes a session key for decrypting the response;

17 the response is a boundary license;

18 the key included in the response is a boundary key for decrypting the  
19 content license;

20 the content license includes a content key;

21 the content key is for decrypting the encrypted content; and

22 the playback application is executable to:  
23

24 decrypt the session license using the client key to obtain the session  
25

key;

decrypt the boundary license using the session key to obtain the boundary key;

decrypt the content license using the boundary key to obtain the content key; and

decrypt the content using the content key.

29. (original): A client as described in claim 23, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

30. (original): A client as described in claim 23, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

31. (original): A client as described in claim 23, further comprising a tuner configured to receive the encrypted content when streamed over a network.

1 32. (original): A client as described in claim 23, wherein the license  
2 includes a certificate for verifying the licensing server.

3  
4 33. (original): A system comprising:

5 a network;

6 a client including:

7 a persistent license having a key that is encrypted; and

8 a playback application that is executable to:

9 form a request to access encrypted content, wherein the  
10 request includes the persistent license;

11 receive a response to the request that includes the key; and

12 access the encrypted content utilizing the key; and

13 a licensing server including a licensing module that is executable to:

14 receive the request including the persistent license;

15 decrypt the persistent license to obtain the key; and

16 form the response that includes the key for communication to the  
17 client over the network.  
18  
19

20  
21 34. (original): A system as described in claim 33, wherein:

22 the client includes a content license;

23 the key included in the persistent license is for decrypting the content  
24 license;  
25

1 the content license includes a content key; and  
2 the content key is for decrypting the encrypted content.

3  
4 35. (original): A system as described in claim 33, wherein:

5 the client includes a content license;

6 the key included in the persistent license is for decrypting the content  
7 license;

8 the content license includes a content key;

9 the content key is for decrypting the encrypted content; and

10 the playback application is executable to:

11 decrypt the content license utilizing the key to obtain the content  
12 key; and

13 decrypt the content utilizing the content key.  
14

15  
16 36. (original): A system as described in claim 33, wherein:

17 the client includes a session license, a content license, and a client key;

18 the client key is for decrypting the session license;

19 the session license includes a session key for decrypting the response;

20 the response is a boundary license;

21 the key included in the response is a boundary key for decrypting the  
22 content license;  
23

24 the content license includes a content key; and  
25

1 the content key is for decrypting the encrypted content.

2  
3 37. (original): A system as described in claim 33, wherein:

4 the client includes a session license, a content license, and a client key;

5 the client key is for decrypting the session license;

6 the session license includes a session key for decrypting the response;

7 the response is a boundary license;

8 the key included in the response is a boundary key for decrypting the  
9 content license;

10  
11 the content license includes a content key;

12 the content key is for decrypting the encrypted content; and

13 the playback application is executable to:

14 decrypt the session license utilizing the client key to obtain the  
15 boundary key;

16 decrypt the boundary license utilizing the session key to obtain the  
17 boundary key;

18 decrypt the content license utilizing the boundary key to obtain the  
19 content key;

20 decrypt the content utilizing the content key; and

21 play the decrypted content.  
22  
23

24 38. (original): A system as described in claim 33, wherein the key is for  
25

1 decrypting the encrypted content.

2  
3 39. (original): A system as described in claim 33, wherein the persistent  
4 license is encrypted with an asymmetric encryption algorithm and the server  
5 includes a server private key for decrypting the persistent license.

6  
7 40. (original): A system as described in claim 33, wherein the playback  
8 application is further executable to:

9 form an initial request for:

10 communication to the licensing server; and

11 storing encrypted content by the playback application;

12 receive the persistent license in response to the initial request; and

13 store the encrypted content and the persistent license.  
14

15  
16 41. (original): A system as described in claim 33, wherein the playback  
17 application is further executable to form a request to obtain the encrypted content  
18 from another client.  
19

20  
21 42. (original): A system as described in claim 33, wherein the encrypted  
22 content is streamed to the client over the network.  
23  
24  
25